9-10-04

Express Mail No. EV528708610US

Attorney Docket No. 108298627US
Disclosure No. MUEI-0533.00/US

TRANSMITTAL OF APPEAL BRIEF	Docket No. 108298627US

In re Application of: Kurt Clement

Application No.	Filing Date	Examiner	Group Art Unit
09/518,787 - Conf. No. 7353	March 3, 2000	James A. Reagan	3621

Invention: SOFTWARE DISTRIBUTION METHOD AND APPARATUS

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed: June 10, 2004 .

The fee for filing this Appeal Brief is 330.00 .

[X] Large Entity [ ] Small Entity

[X] A check in the amount of 330.00 is enclosed.
[X] A check in the amount of 110.00 is enclosed.

[ ] Charge the amount of the fee to Deposit Account No. _____ .
This sheet is submitted in duplicate.

[ ] Payment by credit card. Form PTO-2038 is attached.

[X] The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 50-0665 .
This sheet is submitted in duplicate.

Dated: September 9, 2004

Stephen E. Arnett
Attorney Reg. No.: 47,392
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000

Express Mail No. EV528708610US

Attorney Docket No. 108298627US
Disclosure No. MUEI-0533.00/US

(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kurt Clement

Application No.: 09/518,787 Conf. No.: 7353

Filed: March 3, 2000 Art Unit: 3621

For: SOFTWARE DISTRIBUTION METHOD AND APPARATUS Examiner: James A. Reagan

APPELLANT'S BRIEF UNDER 37 C.F.R. § 1.192

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is hereby filed in furtherance of the Notice of Appeal filed in this case on June 10, 2004. The fee required under 37 C.F.R. § 1.17(c), and a petition for an extension of time and the associated fee, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate.

This brief contains items under the following headings, as required by 37 C.F.R. § 1.192 and MPEP § 1206:

I. Real Party In Interest
II Related Appeals and Interferences
III. Status of Claims
IV. Status of Amendments
V. Summary of Invention
VI. Issues

[10829-8627/SL042460.246]

VII. Grouping of Claims
VIII. Argument
IX. Appendix: Claims Involved in the Appeal

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Micron Technology, Inc., the owner of the present application.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

There are 29 claims pending in the application. No claims were cancelled or withdrawn during prosecution. Claims 1-29 stand rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

The claims have not been amended subsequent to the final rejection in the Final Office Action dated February 10, 2004.

V. SUMMARY OF INVENTION

Digital data products include computer software applications, data files, artistic and informational recordings, and the like. Such products are typically distributed to end users in one of two ways. The first way involves storing the digital data on a recording media and distributing the media to end users through conventional retail channels. This approach has the downside of requiring suppliers and retailers to bear the cost of the time value of money while inventory sits on their shelves. Another method for distributing these products is to enable users to download electronic copies of the information over a

network, such as a local or wide area network, or the Internet. Distribution by downloading, however, can be relatively time-consuming and inconvenient because of the relatively low bandwidth of the network. The inconvenience of downloading can discourage some users from purchasing the related product. (P. 2, ll. 3-16).

A number of products attempt to solve the distribution problems outlined above. One such product is the "Type on Call" product distributed by Adobe Systems, Inc. Type on Call is a CD-ROM that contains many different fonts. The CD-ROM is distributed to end users through conventional channels, and the end users must then contact and pay Adobe Systems, Inc. in order to receive a code necessary to activate one or more of the fonts. This approach has the disadvantage of requiring conventional distribution channels for the CD-ROM, and the further disadvantage of requiring the user to request an access code. (P. 2, ll. 23-28).

The email, network, and Internet service provider America Online, Inc. ("AOL") uses various methods to distribute its access software. One method is to distribute the software for free, and then charge the consumer for subsequent access to the AOL network. The software is provided free of charge, because the value is in the associated access service provided by AOL. A downside of the AOL model, however, is that it still requires use of traditional channels to distribute the software. In addition, accessing digital data over the Internet can still take a relatively long time, as compared to accessing data stored locally on a user computer. (P. 3, ll. 1-9).

Several embodiments of the present invention are directed to methods and systems for distributing software with a computer system to an end user. In one claimed embodiment, a method for distributing software includes recording data on a hard disk, optical disk, programmable read-only memory, or other fixed medium. (P. 6, ll. 1-7, and Figure 2). The method then includes transferring a computer system containing the fixed medium to a user. The user may be an end user, such as a consumer, or a reseller. (P. 6, ll. 24-25, and Figure 2). Once the computer system has been transferred to the user,

access to the data is controlled by execution of computer code that implements authorization procedures. (P. 6, ll. 25-29, and Figure 2).

In the embodiment illustrated in Figure 3, the authorization procedures begin when a request to use the software application is first detected. (P. 7, ll. 2-4, and Figure 3). Next, the code automatically connects to the Internet or other network and presents a query to a party authorized to grant access to the software application. (P. 7, ll. 9-12, and Figure 3). If the party grants access to the software application, the user can access the data based on the authorization. In addition, the authorization is recorded in the software module, or in a location in the computer system that the software module can query. Thus, if the user attempts to access the data a second time, access will be granted based on the authorization recorded in the user's computer system. However, if the user is not authorized to access the data, access may be interrupted, or the function of the data may be disabled. Alternatively, the user may be presented with an opportunity to set up an account so that future access to the data will be granted. (P. 7, ll. 22-28).

As described above, embodiments of the present invention are directed to methods and systems that provide software applications and other digital data to end users in a relatively quick and easy manner. In this way, end users are encouraged to "impulse buy" software applications that they might otherwise forgo. For example, if a user develops a data processing need after purchasing a computer system, the user can easily activate a software application already loaded into his or her computer system to meet the need. Once activated, the system would automatically establish, or assist the user in establishing, the user's access permissions. Hence, embodiments of the present invention provide significant advantages over the traditional approaches of traveling to a retail outlet to buy the software application, mail-ordering the software application, or downloading the software application. Further, because embodiments of the present invention provide for delivery of digital data on a fixed medium in an originally manufactured computer system, there are no additional shipping or inventory costs associated with delivery of the data. (P. 8, l. 16 to P. 9, l. 2).

VI. ISSUES

A. Whether U.S. Patent No. 5,438,508 to Wyman ("Wyman") and the admitted information about AOL in the Background section of the present application disclose recording a data access authorization in the same computer system in which the data is stored, as required to support a *prima facie* case of obviousness.

B. Whether Wyman and the admitted information about AOL in the Background section of the present application provide the teaching or suggestion to make the claimed combination and the reasonable expectation of success, as required to support a *prima facie* case of obviousness.

VII. GROUPING OF CLAIMS

In the Final Office Action dated February 10, 2004 ("Final Office Action"), claims 1-29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wyman in view of applicant's own admission regarding AOL in the Background section of the present application. For purposes of this appeal only, claims 1-29 are grouped together for analysis and argument.

VIII. ARGUMENT

A *prima facie* case of obviousness requires, *inter alia*, that the prior art references teach or suggest *all* the claimed features. (MPEP § 706.02(j)). In the present case, the prior art references do not teach or suggest all the claimed features. For example, all the pending claims include, *inter alia*, the feature of recording a data access authorization *in the same computer system* in which the data is stored. As explained in greater detail below, however, neither Wyman nor the admitted information about AOL teaches or suggests this feature. Therefore, the Examiner has failed to establish a *prima facie* case of obviousness with respect to claims 1-29 for at least this reason.

A. Whether Wyman and Applicant's Own Admission Regarding AOL Disclose Recording a Data Access Authorization in the Same Computer System in Which the Data Is Stored

Claims 1-29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wyman in view of applicant's own admission regarding AOL in the Background section of the present application. As discussed in detail below, independent claims 1, 10, and 21 all include the feature of recording an authorization to access data *in the same computer system* in which the data is stored. Wyman does not teach or suggest this feature. In contrast, Wyman explicitly teaches recording a temporary license *in a remote license server*. Further, the brief discussion about AOL in the Background section of the present application does nothing to fill the void in Wyman. Simply put, the mere statement that AOL "distributes free media containing its access software" (p. 3, l. 3) cannot reasonably be construed to teach or suggest that AOL then controls access to its software by recording an authorization in the user's computer system. This is especially true in light of the notoriously well-known fact that, as clearly explained in the Background section of the present application, *AOL does not control access to its software*, but instead "subsequently charges consumers for access *to its connections and network*." (P. 3, ll. 3-4) (emphasis added).

1. Claim 1 Is Directed to a Method of Distributing Software With a Computer System That Includes, *Inter Alia*, Recording a Data Access Authorization *in the Computer System*

Claim 1 is directed to a method of distributing software with a computer system. The method includes, *inter alia*, recording data on a fixed medium in the computer system and providing for transfer of the computer system to a user. The method further includes controlling access *to the data in the computer system* by contacting a party authorized to grant access when a first request for access is received. If the party authorizes access to the data, then the authorization is recorded *in the computer system* and access to data already in the computer system is granted based on the recorded authorization. When a

second request for access to the data is received, access is granted based on the authorization previously recorded *in the computer system.*

Independent claim 10 is directed to a software module in a computer system that controls access to a software application stored on a fixed medium in the computer system. The software module verifies authority to access the software application by, *inter alia*, contacting a party authorized to grant access to the software application. If the party provides authorization to grant access to the software application, the authorization is recorded *in the computer system* and access is granted based on the recorded authorization. When subsequent use of the software application is detected, access is granted based on the authorization recorded *in the computer system.*

Independent claim 21 is directed to a computer system operable to provide controlled access to a software application stored on a fixed medium in the computer system. The computer system includes, *inter alia*, a software module that responds to a first activation of the software application by contacting a party authorized to grant access to the software application. If the party provides authorization to grant access to the software application, the software module records the authorization *in the memory of the computer system.* When subsequent activation of the software application is detected, access is granted based on the authorization recorded *in the memory of the computer system.*

2. Wyman Is Directed to a License Management System for a Distributed Computer System That Stores Licenses (Product Use Authorizations) *on a Remote License Server*

As the first sentence of the Wyman Abstract clearly states, Wyman is directed to a "license management system" for use in a "distributed computer system." In Wyman, the licenses are stored on a *remote server computer*, and each product makes a call to the *remote server computer* "upon start-up" (i.e., *each time* the product is started) to determine whether use is permitted. Quoting from Wyman:

> The license server maintains a store of the licenses, called product use authorizations, that it administers. *Upon receiving a call from a user*, the license server checks the product use authorization to determine if the particular use requested is permitted, and, if so, *returns a grant to the requesting user node. The license server maintains a database of product use authorizations* for the licensed products, and accesses this database . . . when a request is received from a user.

(Wyman at col. 6, ll. 57-66) (emphasis added).

3. Applicant's Admission Regarding AOL Teaches That AOL Does Not Control Access to Its Free Internet Access Software, but Only Controls Access to the Related Service

In the Background section of the present application, applicant notes that "AOL sometimes directly distributes free media containing its access software, and subsequently charges consumers for access to its connections and network." (P. 3, ll. 2-4). Applicant goes on to explain, however, that one downside of the AOL model is that "it still requires traditional distribution of media or a relatively slow download." (P. 3, l. 7). In addition, applicant points out that with AOL, "*access to the software is not controlled.* The access control is with regard to the associated service." (P. 3, ll. 8-9) (emphasis added).

4. Wyman and Applicant's Own Admission Regarding AOL Do Not Disclose Recording a Data Access Authorization in the Same Computer System in Which the Data Is Stored

Independent claims 1, 10, and 21 all include the feature of recording a data access authorization *in the same computer system* in which the data is stored. In contrast, Wyman explicitly teaches recording data access authorizations (i.e., "licenses") *in a remote license server.* To support his rejection of claims 1, 10, and 21, however, the Examiner has chosen to ignore this explicit teaching of Wyman, and instead construe the "handle" taught by Wyman as the claimed data access authorization. Specifically, the Examiner states:

> With regard to the newly added limitations of recording authorizations within the user computer system, Wyman . . . discloses storing the authorization handle on the client computer for future reference.

(Final Office Action at 6).

The handle taught by Wyman, however, *is not* a data access authorization. Indeed, as Wyman explains, the handle merely identifies the allocation grant created by a previous call to the license server. By using a handle, a subsequent request for access is expedited by the server because the handle identifies the allocation granted during a previous call. (Wyman at col. 22; ll. 14-36). This definition of "handle" is consistent with its common meaning. For example, the Compaq® Fortran Language Reference Manual defines a "handle" in its glossary as:

> A value (often, but not always, a 32-bit integer) that identifies some operating system resource, for example, a window or a process. The handle value is returned from an operating system call when the resource is created; your program then passes that value as an argument to subsequent operating system routines to identify which resource is being accessed.

(*See* Compaq® Fortran Language Reference Manual at http://h18009.www1.hp.com/fortran/docs/lrm/lrm-frames.html).

As Wyman further explains, "[i]f *the handle* is valid, *the authorization* for this product is retrieved *from the [server] database 23*." (Wyman at col. 23, ll. 66-67) (emphasis added). Thus, the handle of Wyman *cannot* be construed as a data access authorization for the additional reasons that (1) Wyman explicitly teaches that the "handle" and the "authorization" are two different things, and (2) the "authorization" is stored in the server database, whereas the "handle" is stored on the user computer.

In fact, elsewhere in the Final Office Action, the Examiner appears to acknowledge that the handle taught by Wyman cannot be construed as the data access authorization of the pending claims. Specifically, the Examiner states: ". . . Wyman does not specifically disclose an authorization per se recorded on the user's hard drive." (Final Office Action at 3, ¶ 6).

To overcome this shortfall, however, the Examiner goes on to state:

> . . . [o]ne of ordinary skill in the art [would] conclude that it is an obvious modification to store authorization data on a hard drive in light of AOL's technique of preloading software onto a computer before the computer [is] shipped to [a] user and Wyman's use of storing an authorization handle on the computer's hard drive.

(Final Office Action at 3, ¶ 6).

This unsupported assertion is insufficient to form the basis of a *prima facie* obviousness rejection for a number of reasons. First, the MPEP requires that the *applied references* teach or suggest all the features of the pending claims. (MPEP § 706.02(j)). Even assuming (and applicant expressly does not) that there was some motivation *in the prior art* to combine Wyman with the AOL reference, the resulting combination would still fail to produce the claimed invention because neither of these references teaches nor suggests the access authorization feature of the pending claims. For example, even when Wyman and the AOL reference are combined, the remote server in Wyman must still be accessed via a network to obtain the "authorization" to use the licensed software. The Examiner cannot dispense with the MPEP requirement that at least one reference teach the claimed feature by simply stating that "one of ordinary skill in the art [would] conclude that it is an obvious modification" to provide the missing feature.

Second, the proper legal standard for a *prima facie* obviousness rejection is not whether "one of ordinary skill in the art [would] conclude that it is an obvious modification" to produce the claimed invention. Rather, the proper legal standard includes, *inter alia*, whether the teaching or suggestion to make the claimed combination and the reasonable expectation of success are both found in the prior art, and not in applicant's disclosure. (MPEP 2143). Here, regardless of what the Examiner believes one of ordinary skill "[would] conclude" with hindsight of applicant's disclosure, the Examiner has still failed to identify *where the prior art* teaches or suggests making the claimed combination.

For the reasons set forth above, the applied references fail to teach or suggest all the claimed features including, *inter alia*, recording a data access authorization in the same computer system in which the data is stored. Therefore, the Examiner has failed to establish a *prima facie* case of obviousness with respect to claims 1, 10, and 21 for at least this reason.

B. Whether Wyman and Applicant's Own Admission Regarding AOL Provide the Teaching or Suggestion to Make the Claimed Combination and the Reasonable Expectation of Success

In addition to the requirement that the applied references teach or suggest all the claimed features, the MPEP also requires that the "teaching or suggestion to make the claimed combination, and the reasonable expectation of success, must both be found *in the prior art and not based on applicant's disclosure*." (MPEP § 706.02(j)) (emphasis added). In this regard, the MPEP explicitly instructs the Examiner to "set forth in the Office Action . . . an explanation why one of ordinary skill in the art at the time the invention was made would have been motivated to make the proposed modification." (MPEP § 706.02(j)).

In the present case, even assuming (and applicant expressly does not) that the applied references do teach all the claimed features, the Examiner still has not complied with the MPEP and (1) identified where *the prior art* suggests combining the AOL reference with Wyman or (2) set forth an explanation why one of ordinary skill in the art *at the time the invention was made* would have been motivated to make the proposed modification. Instead, all the Examiner states in this regard is:

> [I]t is an obvious modification to store authorization data on a hard drive in light of AOL's technique . . . and Wyman's use of storing an authorization handle. . . ."

(Final Office Action at 3, ¶ 6).

Here, the fact that the Examiner states "it *is* an obvious modification," rather than the legal standard of "it *would have been* an obvious modification at the time the invention

was made" suggests that the Examiner is using impermissible hindsight analysis to mold the applied references into the claimed invention. Regardless, the cursory statements about "AOL's technique" and "Wyman's use of storing an authorization handle" still fail to satisfy the basic requirements for a *prima facie* obviousness rejection for at least the reason that these statements say nothing of substance about *where the prior art references* actually suggest the claimed combination. Absent a suggestion in the prior art, the Examiner has failed to establish a *prima facie* case of obviousness.

In an apparent attempt to provide further support for his assertion that the claimed invention is obvious, the Examiner goes on to state:

> It would be of little burden or consequence to the public to modify these techniques to store a complete authorization on a user's computer.

(Office Action at 3, ¶ 6).

Applicant expressly disagrees with this statement. But more importantly, the proper legal standard for obviousness is not whether "[i]t would be of little burden . . . to the public to modify" the prior art to produce the claimed invention. To the contrary, as set forth above, the proper legal standard includes, *inter alia*, (1) whether the applied references teach or suggest *all* the claim features, and (2) whether the teaching or suggestion to make the claimed combination and the reasonable expectation of success are both found *in the prior art*. (MPEP § 706.02(j)). In the present case, as further set forth above, the applied references do not teach or suggest all the claimed features. Furthermore, even if they did, the Examiner has still failed to identify where the prior art, at the time the invention was made, suggests combining the references and/or modifying them to produce the claimed invention. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness with respect to claims 1, 10, and 21.

Claims 2-9 depend from base claim 1, claims 11-20 depend from base claim 10, and claims 22-29 depend from base claim 21. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness with respect to dependent claims 2-9, 11-20,

and 22-29 for at least the reasons discussed above with regard to the Section 103 rejection of the corresponding base claims, and for the additional features of these dependent claims.

C. Summary

The Examiner has improperly rejected claims 1-29 because the Examiner has failed to establish a *prima facie* case of obviousness. More specifically, the Examiner has (1) failed to provide prior art references that disclose all the features of the claims and (2) failed to provide a teaching or motivation—in the prior art—to modify the references or combine reference teachings. Accordingly, the Appellant respectfully requests that the Board reverse the rejection of claims 1-29.

IX. CLAIMS INVOLVED IN THE APPEAL

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-0665, under Order No. 108298627US, from which the undersigned is authorized to draw.

Dated:

Respectfully submitted,

By_____
Stephen E. Arnett
Registration No.: 47,392
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000
(206) 359-7198 (Fax)
Attorney for Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/518,787

1. (Previously Presented) A method of distributing software with a computer system to a user comprising the acts of:

recording data on a fixed medium in the computer system;

providing for transfer of the computer system to the user; and

controlling access to the data in the computer system by:

in response to receiving a first request for access to the data, contacting a party authorized to grant access to the data;

if the party provides authorization to grant access to the data, recording the authorization in the computer system and granting a first access to the data based on the recorded authorization; and

in response to receiving at least a second request for access to the data, granting a second access to the data based on the authorization recorded in the computer system.

2. (Original) The method of distributing software of claim 1 wherein the act of recording data on the fixed medium includes recording software application program instructions on the fixed medium.

3. (Original) The method of distributing software of claim 2 wherein recording software application program instructions on the fixed medium includes recording software application program instructions that enable a software application that does not depend on continued access to a network for fully functional operation.

4. (Original) The method of distributing software of claim 1 wherein the act of recording data on the fixed medium includes recording data on a hard disk drive.

5. (Original) The method of distributing software of claim 1 wherein the act of controlling access to the data includes the computer system automatically executing computer readable instructions to contact a party authorized to grant access to the data.

6. (Original) The method of distributing software of claim 5 wherein executing computer readable instructions includes executing instructions to activate a network link.

7. (Original) The method of distributing software of claim 5 wherein executing computer readable instructions includes executing instructions to activate access to the Internet.

8. (Original) The method of distributing software of claim 1 wherein the act of controlling access to the data includes determining if a user has a sufficient account credit to continue access to the data.

9. (Original) The method of distributing software of claim 1 wherein the act of controlling access to the data includes determining if a user should be billed for accessing the data.

10. (Previously Presented) A software module used in a computer system operable to provide controlled access to a software application being stored on a fixed medium in the computer system and being distributed with the computer system, the software module operating by:

detecting a first use of the software application on the computer system;

in response to detecting the first use, verifying authority to access the software application by:

contacting a party authorized to grant access to the software application; and

if the party provides authorization to grant access to the software application, recording the authorization in the computer system;

granting a first access to the software application based on the recorded authorization;

detecting at least a second use of the software application on the computer system; and

in response to detecting the second use, granting a second access to the software application based on the authorization recorded in the computer system.

11. (Original) The software module of claim 10 wherein the software application does not depend on continued access to a network for fully functional operation.

12. (Original) The software module of claim 10 wherein the software module and the software application are stored on the computer system during manufacture of the computer system.

13. (Original) The software module of claim 10 wherein verifying authority to access the software application verifies authority of a particular user to access the software application.

14. (Original) The software module of claim 10 wherein verifying authority to access the software application verifies authority of an accessing computer system to access the software application.

15. (Original) The software module of claim 10 wherein verifying authority to access the software application is accomplished through a network connection.

16. (Original) The software module of claim 10 wherein verifying authority to access the software application is accomplished through an Internet interface.

17. (Previously Presented) The software module of claim 10 further comprising:

if authority is verified, then allowing uninterrupted access to the software application; and

if authority is not verified, then interrupting access to the software application.

18. (Original) The software module of claim 17 wherein if authority to access the software application is not verified, then the user is presented with an opportunity to qualify for access to the software application.

19. (Original) The software module of claim 18 wherein the opportunity to qualify for access to the software application includes generating a request to set up an account.

20. (Original) The software module of claim 17 wherein if authority to access the software application is not verified, then the user's access to the software application is terminated.

21. (Previously Presented) A computer system operable to provide controlled access to a software application stored on a fixed medium in the computer system and distributed with the computer system comprising:

a processor;

a memory coupled to the processor; and

a software module executable on the processor and the memory, the software module being responsive to a first activation of the software application by:

contacting a party authorized to grant access to the software application; and

if the party provides authorization to grant access to the software application, recording the authorization in the memory and granting a first access to the software application based on the recorded authorization;

the software module being further responsive to at least a second activation of the software application by granting a second access to the

software application based on the authorization recorded in the memory.

22. (Original) The computer system of claim 21 wherein the accessed software application does not depend on continued access to a network for fully functional operation.

23. (Original) The computer system of claim 21 wherein verifying authority to access the software application verifies authority of a particular user to access the software application.

24. (Original) The computer system of claim 21 wherein verifying authority to access the software application verifies authority of an accessing computer system to access the software application.

25. (Original) The computer system of claim 21 wherein verifying authority to access the software application is accomplished through a network connection.

26. (Original) The computer system of claim 21 wherein verifying authority to access the software application is accomplished through an Internet interface.

27. (Original) The computer system of claim 21 wherein if authority to access the software application is not verified, then the user is presented with an opportunity to qualify for access to the software application.

28. (Original) The computer system of claim 26 wherein the opportunity to qualify for access to the software application includes generating a request to set up an account.

29. (Original) The computer system of claim 21 wherein if authority to access the software application is not verified, then the user's access to the software application is terminated.